International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, February 2012

IMPLEMENTING A SECURE KEY ISSUING SCHEME FOR COMMUNICATION IN P2P NETWORKS

Mohammed Azharuddin , Annapurna P Patil

Department of Computer Science and Engineering, M.S.Ramiah Institute of Technology, Bangalore-560054, India
azharadhoni@yahoo.com, annapurnap2@yahoo.com

ABSTRACT

Key issuing scheme focuses on the confidentiality maintained in using the secret key for communication in p2p networks. Identity based cryptography (IBC) was introduced into peer-to-peer (P2P) networks recently for identity verification and authentication purposes. However, current IBC-based solutions were not addressing the problem of secure private key issuing. In this paper we propose a novel secure key issuing scheme for P2P networks using IBC. We present an IBC infrastructure setup phase, a peer registration solution using Shamir's (k, n) secret sharing scheme, and a secure key issuing scheme, which adopts key generate centre (KGC) and key privacy authorities (KPAs) to issue private keys to peers securely. This enables the IBC systems to be more acceptable and applicable in real-world P2P networks.

1. BACKGROUND

With its distributed, self-organization and self maintenance nature, P2P networks are extremely vulnerable to a large spectrum of attacks [1], mainly due to the lack of a certification service responsible for peers identity verification and for authentication purposes. Traditional certificate-based public key infrastructure (PKI) was used to solve some of the problems by verifying the authenticity of nodes' identities and issuing public key certificate to each node. However, as the node churn is highly frequent in the P2P network, many nodes that stored certificates may quickly become invalid, hence PKI based security protocol is difficult to be deployed. Besides, each node requires large amounts of space to store public key certificates, which can be difficult to implement in practice.

Furthermore, secured P2P overlay communication is efficient if the overlay nodes have a common, shared key for securing the communication. This is difficult to achieve in dynamic P2P overlay networks, as a new key must be generated every time an overlay node membership change occurs in order to preserve forward secrecy. Compared with the PKI technique, identity based cryptography (IBC) can simplify the key management process in P2P networks significantly. The identity of a peer (e.g., peer identifier or peer geometric coordinate) in P2P overlay networks is used to create its public key, thus avoiding the use of any certificates. These IBC-based systems are scalable, simple to administer, and each user can carry out anytime/anywhere encryption, establish secure communication channels, prove its identity to other nodes, verify protected messages and produce a form of signature with non-repudiation property.

2. INTRODUCTION

Modern cryptography follows a strongly scientific approach, and designs cryptographic algorithms around computational hardness assumptions, making such algorithms hard to break by an adversary. Such systems are not unbreakable in theory but it is infeasible to do so by any practical means. These schemes are therefore computationally secure. There exist information-

DOI : 10.5121/ijwmn.2012.4111

theoretically secure schemes that provably cannot be broken but these schemes are more difficult to implement than the theoretically breakable but computationally secure mechanisms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Since the 1980s, public-key infrastructures(PKIs) have been widely anticipated as a primary means to make entities' keys available to others in a trusted fashion, thereby enabling a qualitative improvement in the protection and assurance of communications and transactions carried out over the Internet. Certificate-based authentication has become common practice in certain contexts, particularly in conjunction with SSLprotected web sites. In recent years, however, many commentators have lamented the fact that PKI has not achieved more pervasive adoption and deployment. Some have concluded that PKI is a failure or does not address users' primary security needs [19].Opinions differ on the reasons for these results, but most can be distilled into a few general categories.

The demand for the services offered by PKI, in terms of PKI-integrated applications and/or security-oriented use cases for those applications, has not yet emerged to a degree sufficient to motivate deployment of a trust infrastructure. A belief that characteristics of current PKI architectures and implementations make them unnecessarily difficult to deploy, and/or that those characteristics render them incapable of delivering value which alternate approaches could achieve[18].

2.1 Related Work

IBC uses the user's identity as the public key. The private keys of the users are issued by a key generate centre (KGC) after verifying the user's credentials. IBC was introduced in 1984 by Shamir [2]; however, the first practical encryption scheme (IBE) was not available until 2001 which was developed by Boneh and Franklin [3]. Though IBC overcomes the problems of the traditional PKI, it suffers from some inherent problems, one of which is the secure channel requirement: key issuing requires secure channel to avoid eavesdropping. In 2001, Boneh and Franklin [3] addressed secure key issuing problem using multiple key issuing authorities. After that, many key issuing protocols [4], [5], [6] without secure channels were proposed.

So far, several studies have been focused on introducing IBC into P2P security applications. Lu et al. in [7] combined distributed hash tables (DHTs [8]) and identity based encryption (IBE) to defend against man-in-the-middle attacks, however, the scheme assumed that each node has had a pre-assigned unique identifier, and has obtained the corresponding private key through a secure offline channel. This is expensive and difficult to achieve in a large scale P2P overlay network. In [9], Lua proposed a hybrid security protocol using IBE to resist the Sybil attacks, Ryu et al. in [10] proposed ID assignment protocols based on IBC to permit the acquisition of node IDs to be tightly regulated in order to mitigate the Sybil attacks, but these two schemes still suffered from the attack against key issuing phase. Likir [11] presented by Aiello et al. signs messages with IBS in Kademlia-based P2P networks, however the authors supposed every system user had already obtained a private key and did not consider the key issuing problem.

In real-world P2P networks, it is important to have a key issuing scheme in order to keep in secret whether the private key corresponding to a certain identity has been requested. In this paper, a secure key issuing scheme for P2P networks, which addresses the shortcomings of [7], [9], [10], [11], and makes IBC more applicable in the real world is presented.

2.2 Contribution

In this paper, a novel secure key issuing scheme for P2P networks is proposed along with the setup scheme of IBC infrastructure. A peer registration protocol which can register peers adopting Shamir's secret sharing scheme is introduced [12].Finally a secure key issuing protocol which can issue private keys securely without the requirement of secure channels is introduced. The protocol enables IBC more acceptable and applicable in real-world P2P networks.

3. DESIGN

We state the assumptions and requirements firstly, then we propose NOVEL KEY ISSUING SCHEME in the following four sections: system setup, peer registration, secure key issuing and system maintenance. System setup section describes how KGC and KPAs work at the beginning of the system. Peer registration section and secure key issuing section describe how a peer joins in the system. Adopting the threshold cryptography to register users, and using secure key issuing scheme to issue private keys. System maintenance section describes the maintenance mechanisms of KPAs .

ID_A :	Peer A's identity (ID)
K_A :	Peer A's private key
$Proof_A$:	Peer A's proof of the registration
$\cdot$	Concatenation
$SS(x,k)$	Secret share of secret x in Shamir's (k,n) threshold secret sharing scheme
$MAC(x,K)$	Keyed message authentication code of data x and key K
$\{X\}K_A$	A string X signed by peer A
$Thres_{KPA}$	Minimum number of KPAs system possesses
$PK_A(ID)$	Partial key of peer ID issued by A
$Pzl(x)$	A puzzle generated using Seed x
$Sln(x)$	Solution of Puzzle x

3.1 Terminology and assumptions

We present the entities involved and the security assumptions for the proposed scheme in this section.

KGC: There is a trusted core node which acts as KGC at the centre of the system, which provides peer registration and key issuing service. We assume that it has been highly fault tolerant and always available.

KPA: n nodes are selected as Key Privacy Authorities (KPAs) in order to provide the key privacy service in the key issuing phase, which are not required to be as reliable as KGC. In addition, malicious attackers can potentially compromise some of these nodes to perform insider attacks.

Peer: A peer is an ordinary node in P2P networks, which is vulnerable to all kinds of attacks.

3.2 Requirements

Secure peer registration: It must provide a method to mitigate attacks such as man-in-the-middle attacks, collusion attacks and DoS attacks during the peer registration phase.

Secure key issuing: It must provide a method to issue keys securely without secure channels during the key issuing phase, and defend against replay attacks, man-in-the-middle attacks and insider attacks.

3.3 System setup

There is one KGC node and n bootstrap KPA nodes at the setup phase. First, KGC selects a master key, publishes its identity (ID) and specifies the system parameters; Secondly, KGC assigns to each bootstrap KPA node an ID and a corresponding private key based on IBC scheme via a secure offline channel. Note that, the secure offline channel is only required in the system bootstrap phase, since with its ID and private key, a KPA can communicate with the KGC through a secure channel established based on IBC.

3.4 Peer registration

Before joining the network, a peer A should get registered to the KGC at first.
A simple protocol employed is as following. The peer A generates a request with a random nonce and sends it to KGC. After KGC receives the request, KGC issues (IDA,ProofA) for A. The proof of registration Proof A is a message that can prove whether the peer has been registered. Assigning ID by KGC can prevent a peer from choosing its own ID, and mitigate the Sybil attack in the system. However, the communication between KGC and A may be intercepted or modified by malicious peers in real-world P2P networks. We adopt Shamir's (k, n) threshold secret sharing scheme [12] to secure this process. To protect the registration data (IDA,ProofA), we divide it into many secret shares, so that if some of the secret shares have been intercepted, A can eventually recover the registration data if at least k secret shares are collected. On the other side, if the adversary also wants to recover the registration data, it has to get sufficient secret shares, which is difficult to achieve if the threshold k is appropriately configured.

The protocol is described as follows:

Step1: A -> KGC N
Step2: KGC ->KPA SS(IDA · ProofA, k),N
Step3: KPA ->A SS(IDA · ProofA, k),N

Request: When the peer A wishes to join the network, it must first get registered from KGC. Finding the KGC can be accomplished by consulting a bootstrap node or using an automatic service discovery mechanism. Then A sends a request to KGC. In order to avoid the replay attacks, A couples the request with a nonce N.

Distribution: After KGC receives the request, it generates IDA and ProofA for A. In particular, ProofA can be a keyed message authentication code of IDA, i.e., ProofA = MAC(IDA,KKGC). After that, KGC divides IDA and ProofA into n secret shares using Shamir's (k, n) threshold secret sharing scheme, and then KGC distributes those n secret shares to n KPAs respectively. KGC can divide IDA and ProofA into n pieces, IDA and ProofA are easily reconstructable from any k pieces, but even complete knowledge of k -1 pieces reveals absolutely no information about IDA and ProofA.

Thus, it is very difficult for the adversary to obtain sufficient secret shares in a P2P network if we divide the registration data and set an appropriate threshold k. Reconstruction: After receiving the secret share from KGC, KPAs send them to A. Upon receiving the messages from a KPA, A first checks the nonce N, if N is different from the one in its original request, it just ignores the message. Then A waits for collecting k secret shares from different KPAs within a predefined time window. After the peer A gets at least k different secret shares, IDA and ProofA can be reconstructed.

A detailed description of reconstruction process can be found in [12]. If the peer does not get sufficient secret shares, it may run the peer registration protocol again later. Since in real-world P2P networks, it is difficult to have all those paths node-disjoint, here KPAs can use approaches (such as [13]) to avoid paths between KPAs and A from node-joint, in order to mitigate eavesdropping and DoS attacks. In practice, many ISPs have a single connection to the Internet and if an eavesdropper is listening at that point, it will hear all of the n shares being transmitted. This kind of attack is usually a rare situation.

3.5 Secure key issuing

After registration phase, a peer obtains its ID. The next step is to describe how KGC issues a private key to a peer securely without the requirement of secure channels, and how a peer constructs its private key securely from the KGC and KPAs. Shamir's secret sharing scheme we used in Section 3.3 can also be utilized here, however, with KGC and KPAs in the system, we can make the key issuing phase more secure. We present a protocol which utilizes IBC secure key issuing schemes [4], [5], [6] below. Those schemes use one KGC and multiple KPAs for issuing the private keys to the users. KPAs participate in the key generation phrase, they assign the joining peer partial private keys. A registered peer can obtain its private key securely by collecting partial private key from KGC and KPAs. Those schemes avoid the need for secure channels, and the adversary who wants to obtain the private key must compromise not only KGC but also many KPAs. In our scheme, Saxena's scheme [6] is followed therefore it can easily be extended to other schemes [4], [5]. Our scheme is described as follows:

Step1: A ->KGC: Request, IDA, ProofA,N
Step2: KGC ->A : Partial key from KGC, N
Step3: A ->KPA : Request, IDA, ProofA,N
Step4: KPA ->A : Partial key from KPA, N

System setup: KGC selects its private key and specifies the system parameters. KPAs collaboratively run a key generation and distribution protocol [6], and share a secret s such that any k KPAs can construct it with their own secret shares.

Peer registration: As the system setup process is updated, in the peer registration process, IDA and ProofA are generated in a new way, but we can still utilize the protocol described in Section 3.3 to secure this process.

Request: A sends a request with its proof of registration as well as a nonce to KGC to obtain the partial private key;

KGC response: On receiving A's request, KGC checks the proof to verify whether A has been registered or not, if the result is positive, KGC responses with a partial private key;

Blind KPA request: After receiving the partial private key from KGC, A randomly selects some KPAs and requests them in parallel to provide key privacy service by sending a request;

KPA response: Each KPA authenticates A and issues a partial private key to it;

Key retrieval: On receiving at least k partial private keys from different KPAs, A combines them and then unbinds the resulting value to produce the private key; The scheme above is secure against replay attacks, man in-the-middle attacks and insider attacks, and more details can be found in [6]. It can easily be incorporated with other secure key issuing schemes such as [4], [5] that use KPAs to protect the private key.

4. IMPLEMENTATION

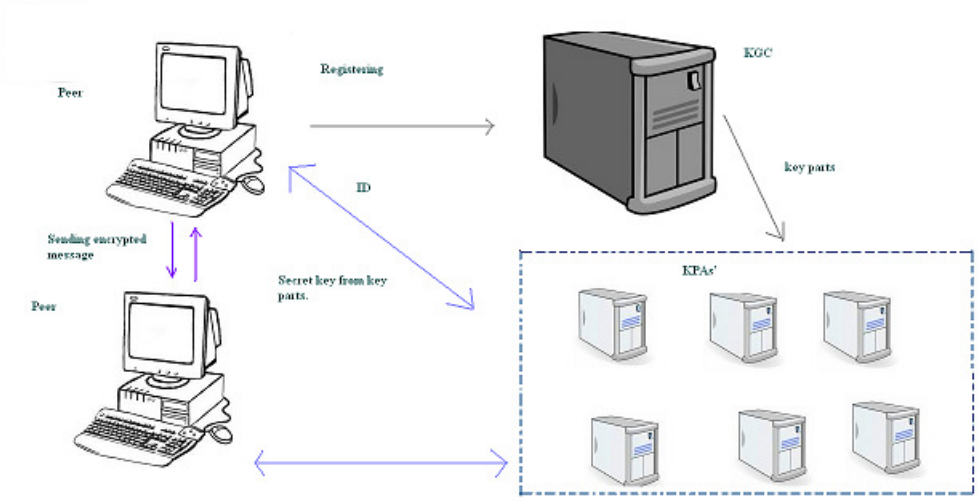

Figure 1: System architecture

The implementation of the key issuing scheme can be as shown by the system architecture in figure 1. The scheme is implemented with six KPAs. The detailed design of our work can be described by following UML design diagrams, which are documented below in Figure 2-5.

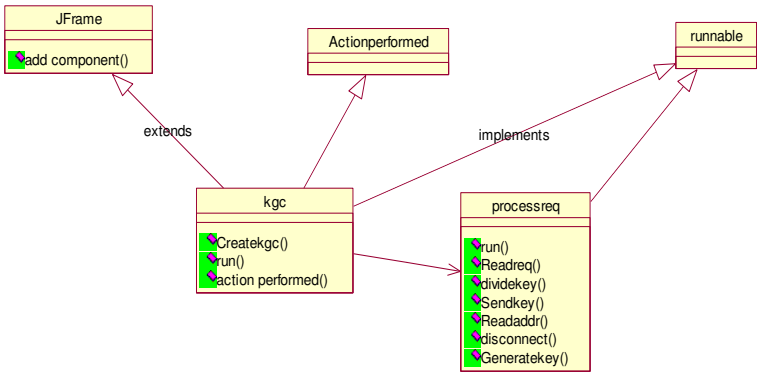

Figure 2: Class diagram for KGC

This is the Key Generation Center (KGC), central node operating in the network.This implements a form of location transparency.The nodes added to the network are unaware of actual location of this central node.This is possible with a level of abstraction provided by the underlying framework. KGC runs as thread on a peer and services the incoming requests by other nodes for registration .It also performs the key generation with the prerequistes of underlying algorithm.It also performs the part of look up work for synthesizing the whole key into parts and back parts into the whole with the mathematical background running over it.

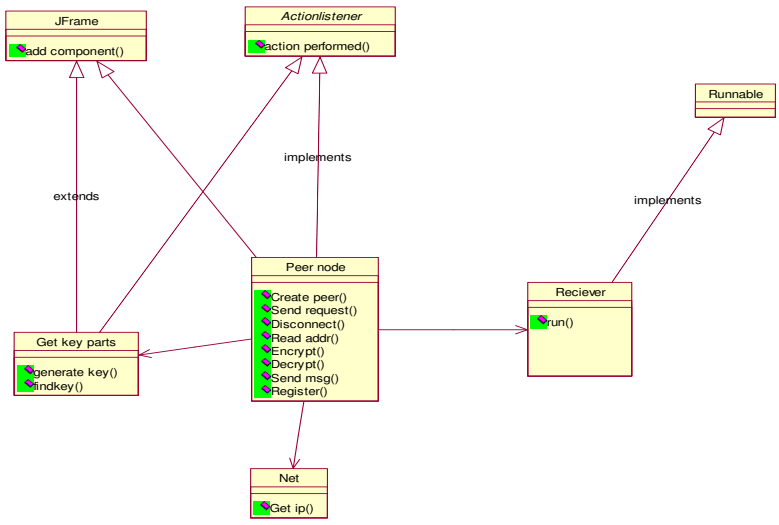

Figure 3: Class diagram for peer node

This is the peer node, a regular node seeking to enter the network and establish the communication with other peer in the network. The peer runs as a thread with different roles. The first form sends a request for registration of node for the communication and awaits the reply token for acquiring the parts of key. The second form is receiver ,which involves rendering the message sent it to it by another peer in the network after unwrapping up of the scrambled data.

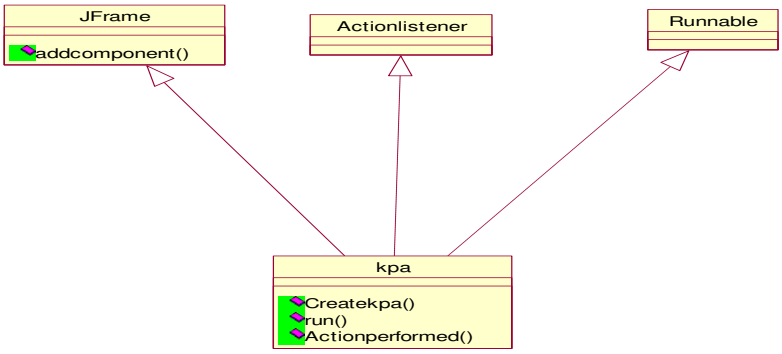

Figure 4: Class diagram for KPA

This is the Key Privacy Authority(KPA).This also runs as a thread. This involves a node in a network , which actually conceals a part of key after it is broken by KGC.The existence of KPAs is solely known to KGC with degree of location transparency and authentication involved.The other peers are unaware of the KPAs . KGC interacts with KPAs after breaking the key.And its upto the peers to render these parts (not all , but subset) with the usage of reference given by KGC.Even if peers come to know the keyparts directly,there is no way of rendering the key without the synthesis process involving the KGC references[2].

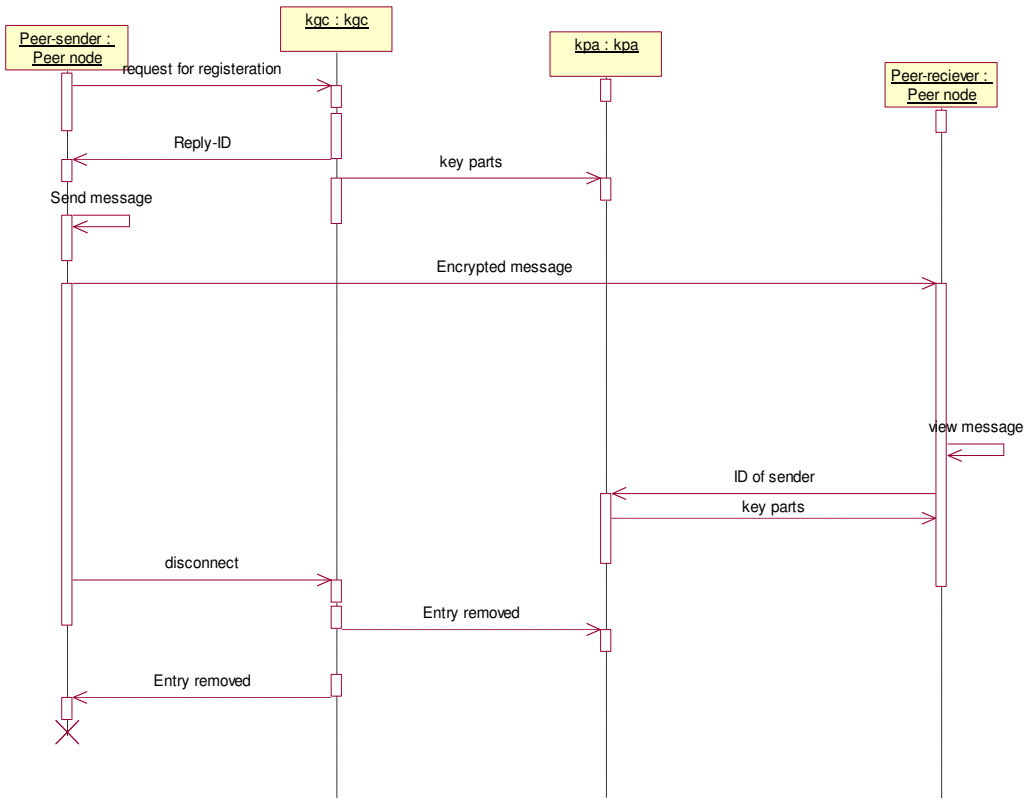

Figure 5: Sequence diagram

The sequence diagram shown above describes the interaction of various modules described with a timeline of events occuring across the network.The initiation of underlying cryptographic process is marked by addition of peer node (sender) in a network and completion by a successful transfer of message with underyling cryptographic process [18].The KGC,KPA are kind of server processes pre running as shown by their early entry in timeline.The process continues with arrival and departure of several peer nodes in a network.

5. CONCLUSION

As the networks are evolving, they also give rise to a requirement of strong security. This feature of networks related to security should be addressed properly. There have been a large number of ways to efficiently handle the security requirement in networks.

Peer to peer networks have a large role in today's fast evolving world and it becomes very essential to manage them efficiently.Security of these networks can be handled on various levels of cryptographic abstractions[1].All these levels have been explored with certain degree of threshold behaviour . In our work we focus on key exchanging phase of a cryptographic schema,where the keys are given to the authenticated nodes involved in communication[12].

In our work we have proposed a novel secure key issuing scheme which is used for basic cryptographic needs such as encryption and decryption. Here we have mainly concentrated on key issuing part of cryptography as previously proposed techniques do not address the issue

effectively. Public Key Infrastructure(PKI) can be used for key issuing however there is problem of managing certificates in PKI as it becomes cumbersome. Hence we go for ID based cryptography, which is efficient compared to PKI.

In this contribution we have implemented a secure key issuing scheme for P2P networks using IBC and have provided a peer registration service using Shamir's secret sharing algorithm. We develop a secure key issuing protocol, which adopts KGC and KPAs to issue private keys to peers securely. The experiments are done on six peers and documented [18].

Our work can be extended to support large scale peer to peer networks of magnitude (10000 peers in simulation environment).It can address Sybil attacks with help of byzantine fault tolerance.

REFERENCES

[1] E. Sit and R. Morris, "Security considerations for peer-to-peer distributed hash tables," in IPTPS, 2002, pp. 261–269.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO, 1984, pp. 47–53.

[3] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001, pp. 213–229.

[4] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Secure key issuing in id-based cryptography," in ACSW Frontiers, 2004, pp. 69–74.

[5] R. Gangishetti, M. C. Gorantla, M. L. Das, A. Saxena, and V. P. Gulati, "An efficient secure key issuing protocol in idbased cryptosystems," in ITCC (1), 2005, pp. 674–678.

[6] A. Saxena, "Threshold ski protocol for id-based cryptosystems," in IAS, 2007, pp. 65–70.

[7] Z.-L. Lu, G.-H.; Zhang, "Wheel of trust: A secure framework for overlay-based services," ICC, pp. 1148–1153, 2007.

[8] I. Stoica, R. Morris, D. R. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in SIGCOMM, 2001, pp. 149–160.

[9] E. K. Lua, "Securing peer-to-peer overlay networks from sybil attack," in ISCIT'07, Sydney, Australia, 2007.

[10] S. Ryu, K. R. B. Butler, P. Traynor, and P. D. McDaniel, "Leveraging identity-based cryptography for node id assignment in structured p2p systems," in AINA Workshops (1), 2007, pp. 519–524.

[11] L. M. Aiello, M. Milanesio, G. Ruffo, and R. Schifanella, "Tempering kademlia with a robust identity based system," in Peer-to-Peer Computing, 2008, pp. 30–39.

[12] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[13] I. Baumgart and S. Mies, "S/kademlia: A practicable approach towards secure key-based routing," in ICPADS, 2007, pp. 1–8.

[14] R. Chen, W. Guo, L. Tang, J. Hu, and Z. Chen, "Scalable byzantine fault tolerant public key authentication for peer-to peer networks," in Euro-Par, 2008.

[15] M. J. Freedman and R. Morris, "Tarzan: a peer-to-peer anonymizing network layer," in CCS, 2002, pp. 193–206.

[16] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. M. Maggs, and Y.-C. Hu, "Portcullis: protecting connection setup from denial-of-capability attacks," in SIGCOMM, 2007, pp. 289– 300.

[17] P. Maymounkov and D. Mazi`eres, "Kademlia: A peer-to-peer information system based on the xor metric," in IPTPS, 2002.

[18] Mohammed Azharuddin and Annapurna P Patil, "Design and Implementation of A secure key issuing scheme for peer to peer Networks",PG Dissertation July 2011,Department of Computer Science and Engineering, M.S.Ramiah Institute of Technology Bangalore-560054,India.

[19] An Examination of Asserted PKI Issues and Pro-posed Alternatives -John Linn, RSA Laboratories, Bedford, MA, USA Marc Branchaud, RSA Security Inc., Vancouver, BC,Canada.